CNS-105-2 Critique #3 : The TESLA broadcast authentication protocol

電機三　徐彥旻　b03901027

Summary

這篇論文處理的是廣播系統的來源認證，意即接收者能夠確認所收到的訊息之來源，以及確認訊息的完整性。這樣的問題之所以重要，是因為雖然衛星、無線電、網路等等的廣播都能夠有效率的傳輸資料，但是卻會讓攻擊者可以偽裝成發送訊息的人。

前人所提出的方法運算量負荷大，使用者有遭受阻斷服務攻擊的疑慮、或是提出的方法能夠容納的接收者數量有限──這都是本篇論文所解決的問題。

只要接收者可以與發送者進行時間同步，並且知道發送者的時間上界，便可以使用這篇論文所提出的 「The TESLA broadcast authentication protocol」。設計者利用 one-way chains 以及金鑰揭露的時間安排，使這個協定能夠達到承受封包遺失、計算量合理等等的廣播認證的需求。

Strengths

利用金鑰揭露的時間的安排──用 one-way chains 產生一系列金鑰，設定時間區間，每個區間用不同的金鑰做出訊息驗證碼──讓對稱式密碼能達成許多非對稱式密碼的性質。比方說確定訊息來源，確保訊息完整性，其他人拿到這個對稱式的密碼卻無法偽造訊息等等。也因為使用的是對稱式密碼，在運算量上也是接收方較能夠負擔的。

Weaknesses

- 訊息發送方可能會受到攻擊者發送大量時間同步請求，或是接收方如果數量龐大，發送方也需要能應付大量的時間同步請求。
- 無法及時驗證訊息，時間間隔設定的愈長、延遲間隔數設定的愈多，就要等待愈久才能驗證。
- 若時間的區間設定的過小，與傳遞延遲的時間接近，則會不安全。

Reflection

在設計協定的時候，接收方、發送方、攻擊者在「什麼時間點」持有「什麼資訊」是可以納入設計當中的。這篇論文便是由此出發，提出了有眾多優點的協定。